Real Roots of Univariate Polynomials and Straight Line Programs

Daniel Perrucci[a,c,*] Juan Sabia[a,b,c,*]

[a] Departamento de Matemática, Facultad de Ciencias Exactas y Naturales,
Universidad de Buenos Aires, Ciudad Universitaria, 1428 Buenos Aires, Argentina

[b] Departamento de Ciencias Exactas, CBC,
Universidad de Buenos Aires, Ciudad Universitaria, 1428 Buenos Aires, Argentina

[c] CONICET - Argentina

Abstract

We give a new proof of the NP-hardness of deciding the existence of real roots of an integer univariate polynomial encoded by a straight line program based on certain properties of the Tchebychev polynomials. These techniques allow us to prove some new NP-hardness results related to real root approximation for polynomials given by straight line programs.

1 Introduction

One of the main problems in real algebraic geometry is to decide whether a system of multivariate polynomial equations has a real root or not. In fact, this problem is equivalent to the one of deciding whether a single polynomial has a real root or not. In the general case, this problem is difficult to solve. The next natural step is to consider the problem for families of polynomials with a particular structure (sparse polynomials or polynomials given by straight line programs, for instance) and to use this particular structure to get a more efficient algorithm for finding the answer to the posed question.

In [5], D. Plaisted showed that the problem of deciding if a univariate sparse integer polynomial has a complex root of modulus 1 is NP-hard (a sparse polynomial is a polynomial codified by a list of exponents including all the non-zero coefficients, plus the list of the coefficients corresponding to these exponents). Later on, Plaisted's result was applied by P. Burgisser to prove that the problem of deciding whether a univariate integer polynomial codified by a straight line program has a real root or not is NP-hard (this proof is unpublished and was told to us by P. Burgisser himself; for a sketch of the proof see [6, Corollary 1]). The proof is obtained by composing the polynomial with a Möbius transformation which sends the real axis to the unitary circumference and by using Plaisted's

*Partially supported by the following Argentinian research grants: UBACyT X112 (2004-2007), UBACyT X847 (2006-2009) and CONICET PIP 5852/05.

result after some little extra work. The same result was obtained by J. Richter-Gebert and U. Kortenkamp in [7, Theorem 5.10] while proving some results in dynamic geometry.

Even though the proofs by Burgisser and in [7] are different, they both rely on a polynomial time reduction of the NP-complete problem 3-SAT to the problem under consideration. More precisely, for a given instance W of 3-SAT, each of the methods shows a construction of a polynomial F with the property that the existence of a real root of F is equivalent to the existence of an interpretation which makes W true. In order to construct this polynomial, they both use factors of polynomials of the type $X^M - 1$ (for some suitable value of M) to codify all the possible interpretations of some predicate symbols $P_1, \ldots, P_n$.

In this paper, we give a new proof of the NP-hardness of deciding whether an integer univariate polynomial codified by a straight line program has a real root or not (see Theorem 7). Our proof is also in the spirit of Plaisted's reduction, but instead of using properties of polynomials of the type $X^M - 1$, we use Tchebychev polynomials in our codification of predicate symbol interpretations. A nice consequence of this approach is that all possible roots of the polynomial we obtain are roots of some Tchebychev polynomial, and this enables us to get a new NP-hardness result concerning the problem of approximating real roots of an integer univariate polynomial codified by a straight line program (see Theorem 9).

The paper is organized as follows: Section 2 states some basic definitions and notations. In Section 3 we give a new proof of the hardness result about the real root existence decision of polynomials codified by straight line programs, even in bounded intervals. In Section 4 we prove the already stated new hardness result for real root approximation.

2 Preliminaries

2.1 Basic definitions and notation

Throughout this paper, we will consider polynomials in $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$, that is, univariate polynomials in a variable X with integer or rational coefficients. For any polynomial $F \in \mathbb{R}[X]$ we will write $\mathrm{lc}(F)$ to denote its leading coefficient.

We will deal with the representation of polynomials by means of *straight line programs* over $\mathbb{Z}$. For a polynomial $F \in \mathbb{Z}[X]$, this codification consists in a program, each of whose instructions is an addition, subtraction or multiplication of two precalculated elements, which enables us to evaluate the polynomial at any given point. The *length* of a straight line program is the number of additions, subtractions and multiplications it performs, even when they just involve elements in $\mathbb{Z}$. Only the variable X and the elements 1 and $-1 \in \mathbb{Z}$ may be introduced without increasing the length of the straight line program. We will write *slp* as a shorthand for "straight line program".

The set of positive (resp. non-negative) integers will be denoted by $\mathbb{N}$ (resp. $\mathbb{N}_0$).

We will call a *literal* any formula in the language of first order of the type P or $\neg P$, where P is a predicate symbol. For $n \in \mathbb{N}$, we will call an *n-clause* a disjunction of n literals.

For the basic notions in complexity theory used in this paper, we refer to [2].

2.2 Tchebychev polynomials

The main objects we will use in our constructions are the *Tchebychev polynomials*, which can be defined recursively as follows:

- $T_0(X) := 1$.
- $T_1(X) := X$.
- For $k \geq 2$, $T_k(X) := 2X\,T_{k-1}(X) - T_{k-2}(X)$.

The following are well known properties of Tchebychev polynomials and can be proved from their recursive definition (see [4], for example). For every $k \in \mathbb{N}_0$:

1. $T_k(X) \in \mathbb{Z}[X]$ is a polynomial of degree k, and, for $k \geq 1$, $\mathrm{lc}(T_k) = 2^{k-1}$.
2. $T_k(x) = \cos(k \arccos(x))$ for $x \in [-1, 1]$. In particular, $T_k(1) = 1$.

As a consequence of these properties, it follows that:

(3) The roots of T_k are the real numbers $\cos(t\pi/2k)$ with t an odd integer between 0 and $2k$. They all lie in the interval $(-1, 1)$ and they all have multiplicity one.

(4) For every $p, q \in \mathbb{N}$, the identity $T_p \circ T_q = T_{pq}$ holds.

From the recursive definition of Tchebychev polynomials and item 4 above, we deduce the following result concerning the complexity of the computation of these polynomials:

Lemma 1 *For every $k \in \mathbb{N}$, the polynomial T_k can be encoded by a straight line program of length $O(k)$. Moreover, if $k = pq$ for some integers $p, q \in \mathbb{N}$, the polynomial $T_k = T_{pq}$ can be encoded by a straight line program of length $O(p + q)$.*

3 Real Roots and Straight Line Programs

This section is devoted to proving the NP-hardness of the problem of deciding the existence of real roots of a univariate polynomial encoded by a straight line program by using the Tchebychev polynomials. We will show that the NP-complete problem 3-SAT can be reduced to this decision problem in polynomial time.

Let us recall first Plaisted's idea in [5] to prove the NP-hardness of deciding if a sparse polynomial has a complex root of modulus 1. The main point is to consider the regular M-gon Q in the complex plane defined by the set of M-th roots of unity. Then, for any prime number p dividing M, consider the regular polygon formed by taking in Q one vertex from each p of them (starting from the vertex at the complex number 1 for every p). Given a way of associating to each predicate symbol in a certain finite set a different prime number dividing M, then each vertex v of Q can be associated to an interpretation $I(v)$ of these predicate symbols in the following way: $I(v)$ makes predicate symbol P_p true if and only if v is a vertex of the polygon associated to prime p. All possible combinations of truth values are realized at the vertices of Q. The main achievement in Plaisted's proof is to assign to any instance W of 3-SAT (and to compute in polynomial time) a sparse polynomial with the property that its only complex roots with modulus 1 (if any) are

exactly those vertices of Q for which its associated interpretation of the predicate symbols makes W true.

Here, we will adapt this construction to a purely real setting. To do so, we will consider a regular polygon with some a priori non-necessary extra vertices, then keep only the upper half of this polygon and consider the projections of the vertices to the real axis. To these real numbers we will associate interpretations of the predicate symbols as explained before.

3.1 Associating a polynomial to a given formula

For $M \in \mathbb{N}$, let us call $d(M)$ the set $\{1, 3, \ldots, 2M-1\}$, i.e, the set of odd integers between 0 and $2M$. For each $t \in d(M)$ we define $r_M(t) = \cos(t\pi/2M)$. Notice that for a fixed M, as t ranges over all the elements in $d(M)$, $r_M(t)$ ranges over all roots of the M-th Tchebychev polynomial T_M and that r_M is 1-1 with its image. Conversely, for each root r of T_M, we denote $t_M(r)$ the unique integer $t \in d(M)$ such that $r = r_M(t)$.

Let q_j be the j-th odd prime number ($q_1 = 3, q_2 = 5, \ldots$). Let W be a well-formed formula of the propositional calculus obtained from predicate symbols $P_j, j = 1, \ldots, n$, using Boolean connectives (including negation). As explained before, to each root r of T_M we associate an interpretation $I_M(r)$ of the predicate symbols $\{P_j \,|\, q_j \text{ divides } M\}$. The interpretation $I_M(r)$ makes the predicate symbol P_j true if and only if r is a root of T_{M/q_j}, and this happens if and only if q_j divides $t_M(r)$.

For every interpretation J of $\{P_j \,|\, q_j \text{ divides } M\}$ there exists at least one root r of T_M such that $I_M(r) = J$, namely $r = r_M(\prod_{j \in K_J} q_j)$ where $K_J = \{j \,|\, J \text{ makes predicate symbol } P_j \text{ true}\}$. As it suffices for our purpose, let us suppose from now on that M is square-free. Then, the set $\{t \in d(M) \mid I_M(r_M(t)) = J\}$ equals the set $\{t \in d(M) \mid \gcd(t, M) = \prod_{j \in K_J} q_j\}$. In this way, each interpretation can be associated with an odd factor $d = \prod_{j \in K_J} q_j$ of M, and with the set of roots which leads us to that interpretation. We will write $\alpha(J) := d$.

Now, we can define the analogue of $\mathrm{Poly}_M(W)$ (as defined in [5]), which will be the main tool in our construction.

Definition 2 *Let M be a square-free integer and W a well-formed formula of the propositional calculus such that for every $j \in \mathbb{N}$, if the predicate symbol P_j occurs in W, then q_j divides M. We define the polynomial* $\mathrm{PolyS}_M(W) \in \mathbb{R}[X]$ *as the monic polynomial having as simple roots the roots r of T_M such that W is true in the interpretation $I_M(r)$.*

We will see later that for every well-formed formula W, $\mathrm{PolyS}_M(W) \in \mathbb{Q}[X]$. Before we continue explaining our reduction, we will need some other definitions and properties.

Let us define an analogue of the cyclotomic polynomials in the following way:

$$\hat{C}_\ell(X) = \prod_{t \in d(\ell),\ \gcd(t:\ell)=1} \Big(X - \cos(\frac{t}{2\ell}\pi)\Big).$$

Then, $\deg \hat{C}_\ell = \phi(2\ell)$, where ϕ is the Euler function. With this definition, it is easy to see that if $\ell \neq \ell'$, then $\hat{C}_\ell(X)$ and $\hat{C}_{\ell'}(X)$ are relatively prime polynomials.

Lemma 3 *Let W be a well-formed formula of the propositional calculus involving the predicate symbols $P_1, \ldots, P_n$. Suppose $M := \prod_{i=1}^n q_i$ or $M := 2\prod_{i=1}^n q_i$ and let $J_1, \ldots, J_k$ be the*

list of the interpretations of the predicate symbols that make W true. Then $\mathrm{PolyS}_M(W) = \prod_{i=1}^{k} \hat{C}_{M/\alpha(J_i)}$.

Proof: Let us show that both polynomials have the same roots. For $1 \leq i \leq k$, the roots of $\hat{C}_{M/\alpha(J_i)}$ are the numbers $r = r_{M/\alpha(J_i)}(t)$ with $t \in d(M/\alpha(J_i))$ such that $\gcd(t, M/\alpha(J_i)) = 1$; but due to the equality $t/(M/\alpha(J_i)) = \alpha(J_i)t/M$, these numbers are exactly those $r = r_M(t')$ with $t' \in d(M)$ such that $I_M(r_M(t')) = J_i$, which are the roots of $\mathrm{PolyS}_M(W)$. □

3.2 Reduction via Tchebychev Polynomials

Here, we will do the reduction of 3-SAT to the problem of deciding the existence of real roots of univariate polynomials codified by slp's. To achieve this, we will prove the following proposition:

Proposition 4 *For any instance W of 3-SAT, it is possible to compute in polynomial time in the size of W a polynomial $F \in \mathbb{Z}[X]$ codified by an slp whose length is polynomial in the size of W with the property that F has the same real roots as* $\mathrm{PolyS}_M(W)$ *for a suitable value of M, and therefore, F has a real root iff W is satisfiable.*

To prove Proposition 4, we will make use of the following lemmas:

Lemma 5 *Let W and W' be well-formed formulae of the propositional calculus, and let M be a square-free integer such that if the predicate symbol P_i occurs either in W or in W', then q_i divides M. Then we have that:*

1. $\mathrm{PolyS}_M(P_{i_1} \wedge P_{i_2} \wedge \cdots \wedge P_{i_l}) = \frac{T_{M/(q_{i_1} q_{i_2} \cdots q_{i_l})}}{\mathrm{lc}(T_{M/(q_{i_1} q_{i_2} \cdots q_{i_l})})}$,
2. *W and W' are equivalent iff* $\mathrm{PolyS}_M(W) = \mathrm{PolyS}_M(W')$,
3. $\mathrm{PolyS}_M(\neg W) = \frac{T_M}{\mathrm{lc}(T_M)\mathrm{PolyS}_M(W)}$
4. $\mathrm{PolyS}_M(W \wedge W') = \gcd(\mathrm{PolyS}_M(W), \mathrm{PolyS}_M(W'))$,
5. $\mathrm{PolyS}_M(W \vee W') = \mathrm{lcm}(\mathrm{PolyS}_M(W), \mathrm{PolyS}_M(W'))$,

Proof: To prove the first item, let us notice that the set of roots of $\mathrm{PolyS}_M(P_{i_1} \wedge P_{i_2} \wedge \cdots \wedge P_{i_j})$ is the set $\{r_M(t) \mid t \in d(M) \text{ and } q_{i_1} q_{i_2} \ldots q_{i_j} | t\}$. This set equals the set $\{r_{M/(q_{i_1} q_{i_2} \cdots q_{i_j})}(t') \mid t' \in d(M/(q_{i_1} q_{i_2} \ldots q_{i_j}))\}$, which is the set of roots of T_{M/q_i}. Items 2-5 are straightforward. □

Note that as a consequence of this lemma, we have the a priori non-obvious consequence that for every well-formed formula W and every suitable M, $\mathrm{PolyS}_M(W) \in \mathbb{Q}[X]$.

To prove Proposition 4, we will also need the following lemma, which will be useful to do the computations:

Lemma 6 *Let W be a well-formed formula of the propositional calculus, and let M be a square-free integer such that if the predicate symbol P_i occurs in W, then q_i divides M. Then we have that:*

1. $\mathrm{PolyS}_M(\neg P_{i_1} \vee \neg P_{i_2} \vee \neg P_{i_3}) = \frac{T_M}{\mathrm{lc}(T_M)\mathrm{PolyS}_M(P_{i_1} \wedge P_{i_2} \wedge P_{i_3})}$,

2. $\mathrm{PolyS}_M(P_{i_1} \vee \neg P_{i_2} \vee \neg P_{i_3}) = \frac{T_M \mathrm{PolyS}_M(P_{i_1} \wedge P_{i_2} \wedge P_{i_3})}{\mathrm{lc}(T_M)\mathrm{PolyS}_M(P_{i_2} \wedge P_{i_3})}$,

3. $\mathrm{PolyS}_M(P_{i_1} \vee P_{i_2} \vee \neg P_{i_3}) = \frac{T_M \mathrm{PolyS}_M(P_{i_1} \wedge P_{i_3})\mathrm{PolyS}_M(P_{i_2} \wedge P_{i_3})}{\mathrm{lc}(T_M)\mathrm{PolyS}_M(P_{i_3})\mathrm{PolyS}_M(P_{i_1} \wedge P_{i_2} \wedge P_{i_3})}$,

4. $\mathrm{PolyS}_M(P_{i_1} \vee P_{i_2} \vee P_{i_3}) = \frac{\mathrm{PolyS}_M(P_{i_1})\mathrm{PolyS}_M(P_{i_2})\mathrm{PolyS}_M(P_{i_3})\mathrm{PolyS}_M(P_{i_1} \wedge P_{i_2} \wedge P_{i_3})}{\mathrm{PolyS}_M(P_{i_1} \wedge P_{i_2})\mathrm{PolyS}_M(P_{i_1} \wedge P_{i_3})\mathrm{PolyS}_M(P_{i_2} \wedge P_{i_3})}$,

5. *If some P_j does not occur in W and $q_j \nmid M$, then* $\mathrm{PolyS}_{Mq_j}(W) = \mathrm{PolyS}_M(W) \circ T_{q_j}$. *If M is odd,* $\mathrm{PolyS}_{2M}(W) = \mathrm{PolyS}_M(W) \circ T_2$.

Proof: Items 1-4 are easy and can be proved using the inclusion-exclusion principle. Let us prove the last item. Let $J_1, J_2, \ldots, J_k$ be the list of all interpretations of all the predicate symbols P_l such that q_l divides M which make W true. For $h = 1, \ldots, k$, let J_h^T be the interpretation that extends J_h to the predicate symbol P_j by making it true. Analogously, we define J_h^F. As P_j does not actually occur in W, the list of all interpretations of all the predicate symbols P_l such that q_l divides M plus P_j which make W true is $J_1^T, J_1^F, \ldots, J_k^T, J_k^F$. Moreover, for $h = 1, \ldots, k$, $\alpha(J_h^T) = q_j\alpha(J_h)$ and $\alpha(J_h^F) = \alpha(J_h)$.

Because of Lemma 3, it is enough to see that for $h = 1, \ldots, k$ it is

$$\hat{C}_{Mq_j/\alpha(J_h^T)}\hat{C}_{Mq_j/\alpha(J_h^F)} = \frac{\hat{C}_{M/\alpha(J_h)} \circ T_{q_j}}{\mathrm{lc}(\hat{C}_{M/\alpha(J_h)} \circ T_{q_j})}.$$

Let us first see that the degrees of both polynomial coincides. The degree of the first polynomial is

$$\phi\big(2Mq_j/\alpha(J_h^T)\big) + \phi\big(2Mq_j/\alpha(J_h^F)\big) =$$
$$= \phi\big(2M/\alpha(J_h)\big) + \phi(q_j)\phi\big(2M/\alpha(J_h)\big) = q_j\phi\big(2M/\alpha(J_h)\big),$$

which is the degree of the second polynomial.

Now, let us take a root r of $\hat{C}_{Mq_j/\alpha(J_h^T)}\hat{C}_{Mq_j/\alpha(J_h^F)}$. Then one of the following possibilities is possible: either $r = \cos(t\pi/(2M/\alpha(J_h)))$ for some $t \in d(M/\alpha(J_h))$ such that $\gcd(t, M/\alpha(J_h)) = 1$ or $r = \cos(t\pi/(2Mq_j/\alpha(J_h)))$ for some $t \in d(Mq_j/\alpha(J_h))$ such that $\gcd(t, Mq_j/\alpha(J_h)) = 1$. These two conditions can be sumarized as $r = \cos(t\pi/(2Mq_j/\alpha(J_h)))$ for some $t \in d(Mq_j/\alpha(J_h))$ such that $\gcd(t, Mq_j/\alpha(J_h)) = 1$ or q_j. Let us see now that any of these values for r is a root of the polynomial on the right hand side of the equality:

$$\hat{C}_{M/\alpha(J_h)}(T_{q_j}(r)) = \hat{C}_{Mq_j/(q_j\alpha(J_h))}\Big(\cos\big(q_j \arccos(\cos(\frac{t}{2Mq_j/\alpha(J_h)}\pi))\big)\Big) =$$

$$\hat{C}_{Mq_j/(q_j\alpha(J_h))}\big(\cos(\frac{t}{2Mq_j/(q_j\alpha(J_h))}\pi)\big) = \hat{C}_{Mq_j/(q_j\alpha(J_h))}\big(\cos(\frac{t'}{2Mq_j/(q_j\alpha(J_h))}\pi)\big),$$

for some $t' \in d(Mq_j/(q_j\alpha(J_h)))$ such that $t \equiv \pm t'(2Mq_j/(q_j\alpha(J_h)))$.

If $\gcd(t, Mq_j/\alpha(J_h)) = 1$, then $\gcd(t, Mq_j/(q_j\alpha(J_h))) = 1$. If $\gcd(t, Mq_j/\alpha(J_h)) = q_j$, as Mq_j is square-free, then again $\gcd(t, Mq_j/(q_j\alpha(J_h))) = 1$. In any case, we know that $\gcd(t', Mq_j/(q_j\alpha(J_h))) = 1$ and then r is a root of $\hat{C}_{M/\alpha(J_h)} \circ T_{q_n}$.

We have proved then that both polynomials have the same roots and therefore they are equal. For the second statement, it can be proved similarly that for any satisfying interpretation of the predicate symbols J,

$$\hat{C}_{2M/\alpha(J)} = \frac{\hat{C}_{M/\alpha(J)} \circ T_2}{\mathrm{lc}(\hat{C}_{M/\alpha(J)} \circ T_2)}$$

and conclude in the same way, using Lemma 3. □

We can now give a proof of Proposition 4:

Proof: Let $\hat{W}$ be a 3-clause involving literals P_{i_1}, P_{i_2} and P_{i_3}, $i_1 < i_2 < i_3 \leq n$. Let $N := q_{i_1}q_{i_2}q_{i_3}$. Due to the fact that $q_i = O(i \log i)$ (see [3, Ch.I]), we know that $\mathrm{PolyS}_N(\hat{W})$ has degree $O(n^3 \log^3 n)$. Using Lemmas 5 and 6, we can compute an slp for a scalar multiple in $\mathbb{Z}[X]$ of this polynomial using the well-known Strassen's Vermeidung von Divisionen (division avoiding) algorithm (see [8]), which computes an slp for the quotient of two polynomials in the following setting: suppose $f_1, f_2 \in \mathbb{Q}[X]$ are codified by slp's of length $O(L)$; if we know that $f_2|f_1$, and we have a bound d for the degree of the quotient $\frac{f_1}{f_2}$ and an element $r \in \mathbb{Q}$ such that $f_2(r) \neq 0$, then we can compute in polynomial time an slp for $\frac{f_1}{f_2}$ with length $O(d^2(d + L))$.

In our case, we have the bound for the degree required, and for each division, we know that the evaluation of the denominator at 1 gives as result 1. This is so because if we unravel the formulae in Lemma 6 without the leading coefficients involved (we can do so because we are interested in computing a scalar multiple of the polynomial $\mathrm{PolyS}_N(\hat{W})$), we have that the denominator is always a product of Tchebychev polynomials. These facts enable us to adapt the Vermeidung von Divisionen procedure to the slp setting in $\mathbb{Z}[X]$ within the same order of complexity. Besides, the length of the slp we obtain is $O(n^9 \log^9 n)$.

Let M be $\prod_{i=1}^n q_i$ or $2\prod_{i=1}^n q_i$ (this second option for M will be useful in the next section). Once we have computed an slp for $\mathrm{PolyS}_N(\hat{W})$, because of the last item of the lemma above we can compute an slp for $\mathrm{PolyS}_M(\hat{W})$ by adding at the beginning of the code for $\mathrm{PolyS}_N(\hat{W})$ the code for T_{q_i} for each prime q_i different from q_{i_1}, q_{i_2} and q_{i_3} (which is the same as making the composition with T_{q_i}) and the code for T_2 if needed. This adds $O(n^2\log(n))$ to the length of our slp. Thus, we can compute in polynomial time an slp for $\mathrm{PolyS}_M(\hat{W})$ with length $O(n^9 \log^9(n))$.

To end our proof, we proceed in the following way. Given any instance W or 3-SAT, involving predicate symbols $P_1, \ldots, P_n$, we take $M = \prod_{i=1}^n q_i$ or $M = 2\prod_{i=1}^n q_i$, and we compute an slp for the sum of the squares of the polynomials $\mathrm{PolyS}_M(\hat{W})$, where $\hat{W}$ ranges over all the 3-clauses appearing in W. We call F the polynomial which is encoded by this slp. If W is a conjunction of m 3-clauses, then this slp codifying F has length $O(mn^9 \log^9(n))$, and F has a real root if and only if there is an interpretation of the predicate symbols which makes W true. □

As a direct corollary of Proposition 4, we have a new proof of the following result:

Theorem 7 *Deciding whether a univariate polynomial codified by a straight line program in $\mathbb{Z}$ has a real root or not is NP-hard.*

Suppose now that we consider the size of a rational number r/s as $\log(|r|) + \log(s)$. As the polynomial F we computed in the proof of Proposition 4 has all its real roots (if any) in the interval $(-1, 1)$, it follows that even with *small* rational endpoints, it is hard in general to decide the real root existence in a given interval. So, again as a direct corollary of Proposition 4, we have a new proof of the following theorem:

Theorem 8 *Deciding if a univariate polynomial codified by an slp in $\mathbb{Z}$ has a root in an interval (a, b) given by $a, b \in \mathbb{Q}$ is NP-hard in the strong sense.*

4 Approximating real roots is NP-hard

In this section we will use the construction we have done in the previous section to get some new results concerning the complexity of the problem of approximating real roots of a univariate integer polynomial encoded by a straight line program. Our main result is:

Theorem 9 *The following two search problems are NP-hard (in the sense of [2, Chapter 5]):*

- *Given a polynomial $F \in \mathbb{Z}[X]$ encoded by a straight line program, an (open, semiopen or closed) interval I with endpoints $a, b \in \mathbb{Q}$ such that F has a root in I, and given $\varepsilon > 0$, find $c, d \in (I \cup \{a, b\}) \cap \mathbb{Q}$ such that $d - c < \varepsilon$ and F has a root in $[c, d] \cap I$.*
- *Given a polynomial $F \in \mathbb{Z}[X]$ encoded by a straight line program, an (open, semiopen or closed) interval I with extremes $a, b \in \mathbb{Q}$ and given $\varepsilon > 0$, find $c, d \in (I \cup \{a, b\}) \cap \mathbb{Q}$ such that $d - c < \varepsilon$ with the property that if F has a root in I, then F has a root in $[c, d] \cap I$.*

Proof: To prove the first item, we will show a polynomial time reduction from the NP-hard problem F3-SAT.

Let W be an instance of 3-SAT formed by m different 3-clauses on the predicate symbols $P_1, \ldots, P_n$ which we know to be satisfiable. Let $M := 2q_1 \ldots q_n$ and let F be the polynomial computed in the previous section whose real roots are precisely those of the polynomial $\mathrm{PolyS}_M(W)$. We have already proved that we can compute in polynomial time an slp of length $L = O(m\, n^9 \log^9(n))$ encoding F. As W is satisfiable, we know that F has a root $r = r_M(t)$ with $r \in (-1, 1)$, for some odd integer $t \in d(M)$. In fact, the factor 2 in M ensures us that there will be at least two such roots, one of them lying in the interval $(-3/4, 3/4)$: if $t \leq M/2$, then $M/2 < t + M \leq 3M/2$ and $I_M(r_M(t)) = I_M(r_M(t + M))$, so we can replace t by $t + M$; analogously, if $t \geq 3M/2$, then $M/2 \leq t - M < 3M/2$ and $I_M(r_M(t)) = I_M(r_M(t - M))$, and we replace t by $t - M$. In any case, we may assume that t is an odd integer between $M/2$ and $3M/2$. We conclude that F has a real root $r_M(t)$ in the interval $[-\sqrt{2}/2, \sqrt{2}/2] \subset (-3/4, 3/4)$.

Note that if $-3/4 < r_1 < r_2 < 3/4$, with $r_1 = \cos(t_1\pi/2M), r_2 = \cos(t_2\pi/2M)$ for some odd integers $t_1 > t_2$ in $d(M)$, then due to the mean value theorem, there exists a real number $\xi \in (\arccos(3/4), \arccos(-3/4))$ such that

$$r_2 - r_1 = \cos(t_2\pi/2M) - \cos(t_1\pi/2M) = \frac{\sin(\xi)(t_1 - t_2)\pi}{2M} \geq \frac{\sqrt{1-(3/4)^2}\pi}{M} > \frac{2}{M}.$$

So, any two distinct possible roots of polynomial F in the interval $(-3/4, 3/4)$ are separated by a distance of at least $2/M$.

As $\log(M) = \Theta(q_n) = O(n)$, where Θ is the Tchebychev function $\Theta(x) = \sum_{p \leq x,\, p \text{ prime}} \log(p)$ (see [3, Ch.XXII, Theorem 415]), we can consider $\varepsilon := 1/2M$, which size is polynomial in n, and suppose that we can find in polynomial time a pair of numbers $c, d \in [-3/4, 3/4] \cap \mathbb{Q}$ with $d - c \leq \varepsilon$ such that F has a real root in $[c, d] \cap (-3/4, 3/4)$.

Since $d - c$ is lower than the minimum separation between distinct roots of F, we conclude that there is exactly one real root $r_0 = r_M(t_0)$ of F in $[c, d]$, and this means that we have an interpretation of the predicate symbols which makes W true. We just need to prove that we can decide in polynomial time for which $t \in d(M)$, the inequalities $c \leq r_M(t) \leq d$ hold.

We proceed in several steps. First we use Bailey, Borwein and Plouffe's formula (see [1]):

$$\pi = \sum_{i=0}^{\infty} \frac{1}{16^i}\Big(\frac{4}{8i+1} - \frac{2}{8i+4} - \frac{1}{8i+5} - \frac{1}{8i+6}\Big),$$

to find an approximation s in $\mathbb{Q}$ to the number π such that $|s - \pi| < 1/4M$ in time polynomial in $\log(M)$. Now, for a given integer t, we can find an estimate s_2 in $\mathbb{Q}$ for $\cos(ts/2M)$ using the Taylor expansion with error bounded by $1/4M$, also in time polynomial in $\log(M)$. We have that $|s_2 - \cos(t\pi/2M)| \leq |s_2 - \cos(ts/2M)| + |\cos(ts/2M) - \cos(t\pi/2M)| \leq |s_2 - \cos(ts/2M)| + |t\pi/2M - ts/2M| \leq 1/2M$.

Note that if for some value of $t \in d(M)$ the approximation s_2 to $\cos(t\pi/2M)$ lies in the interval $[c - 1/2M, d + 1/2M]$, then $t = t_0$, because otherwise $|r_M(t) - r_M(t_0)| \leq |r_M(t) - s_2| + |s_2 - r_M(t_0)| \leq 1/2M + 1/M < 2/M$, which is impossible. Then, using a bisection method in $d(M)$, we compute approximations to $\cos(t\pi/2M)$ for up to $O(\log M)$ distinct numbers $t \in d(M)$ in polynomial time, till we find t_0, which is the first (and only) value such that the approximation lies in $[c - 1/2M, d + 1/2M]$.

In order to prove the second item, we proceed in an analogous way to make a reduction from 3-SAT. If we can find an interval $[c, d] \subset I \cup \{a, b\}$ of length at most ε with the property that if F has a root in I, then F has a root in $[c, d] \cap I$, we apply this algorithm to $F = \text{PolyS}_M(W)$ and $[a, b] = [-3/4, 3/4]$. This leads us to the fact that we just need to evaluate the formula W at one possible interpretation (which can be done in polynomial time) to find a satisfying interpretation of the predicate symbols, if there is one. This proves the second item. □

Acknowledgments

The authors would like to thank Peter Burgisser, Gabriela Jeronimo and the anonymous referees for their helpful comments.

References

[1] D. Bailey, P. Borwein and S. Plouffe, *On the rapid computation of various polylogarithmic constants,* Math. Comp. 66 (1997), 903-913.

[2] M. Garey and D. Johnson, *Computers and Intractability, A Guide to the Theory of NP-Completeness,* W.H. Freeman and Company, New York, 1979.

[3] G. Hardy and E. Wright, *An introduction to the Theory of Numbers,* Fourth Edition, Oxford University Press, Oxford, 1960.

[4] D. Kincaid and W. Cheney, *Numerical Analysis: Mathematics of Scientific Computing,* Brooks/Cole Publishing Company, Belmont, California, 1991.

[5] D. Plaisted, *New NP-Hard and NP-Complete polynomial and integer divisibility problems,* Theoret. Comput. Sci. 31 (1984), 125-138.

[6] M. Rojas, *Algebraic Geometry Over Four Rings and the Frontier to Tractability,* invited paper, Contemporary Mathematics, vol. 270, Proceedings of a Conference on Hilbert's Tenth Problem and Related Subjects (University of Gent, November 1-5, 1999), edited by Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel, pp. 275-321, AMS Press (2000).

[7] J. Richter-Gebert and U. Kortenkamp, *Complexity issues in dynamic geometry.* In: Felipe Cucker and J. Maurice Rojas, editors, Foundations of Computational Mathematics (Proceedings of the Smale Fest 2000). World Scientific, 2002. Also available as technical report TRB-2000/22, Freie

[8] V. Strassen, *Vermeidung von Divisionen,* J. Reine Angew. Math 264 (1973), 182-202.